Global Information Assurance Certification Paper

GIAC Certified Windows Security Administrator Practical Exam

Prepared By:
Jack Green
January 16, 2005

Version 3.1

Securing a Windows 2000 Network for a Small Organization

Abstract

This paper present a Windows 2000 network designed for a small organization that maintains two offices is relatively geographically disparate areas. The designs specifications of this paper were:

- Network security
- Simplicity of management
- Flexibility and ease of granting or restricting network privileges

These goals, described in more detail in the body, were met through group policies, creation of sites and careful planning of Organizational unit structure.

Description of GIAC Enterprises

The market for fortune cookies has exploded in the post-dotcom bubble. GIAC Enterprises (GE). a designer of custom fortune cookie sayings, has experienced commensurate growth in demand for its product.

From its foundations as a small Vermont company, the company has found the need to take its product to larger markets. Corporate headquarters has been located in New York City. Current employees, including the founder/president, at the Stowe, Vermont location are unwilling to move. Consequently the corporation will reorganize in the manner described in Table 1

Location	Department	Logistics	Functions
New York	Sales and Marketing	Sixteen account managers/rep's, two marketing rep's and occasional marketing consultants. Two network support staff. Four staff members responsible for hiring,	Launch product rollouts, coordinate and execute sales calls with customers
	Finance and Human Resources	benefits coordination. CFO is located here as well.	Manage books, staffing and etc..
Stowe	Research and Development	Eight programmers/oracles. One network support member	Maintain a program that generates random computer generated fortunes.
All	IT Staff	Three administrators rotate in and out of New York and Stowe.	Cross-trained to manage the nertwork and workstations at each site.

Table I – Departmental Configuration GIAC Enterprises

Information Technology Situation

GIAC Enterprises decided to commit to the Windows 2000 network operating system in this reorganization. None of the existing NT servers were upgradeable to 2000 specifications. New hardware was purchased providing the staff with the opportunity to run in Native mode.

Network Goals:

1) Network structure and, consequently, management will be as simple as possible.
2) All workstations and users must be secured. Research and Development has different security requirements than the other departments.
3) Management of security policies may be implemented by IT staff at each of the two sites. However, the default domain policy is immutable.
4) Consultants, who are employed on occasion, have additional constraints for network use.
5) Certain non-IT departmental staff will be asked to perform some of the less technical network management tasks.

Network Design and Diagram

Operating system update configuration

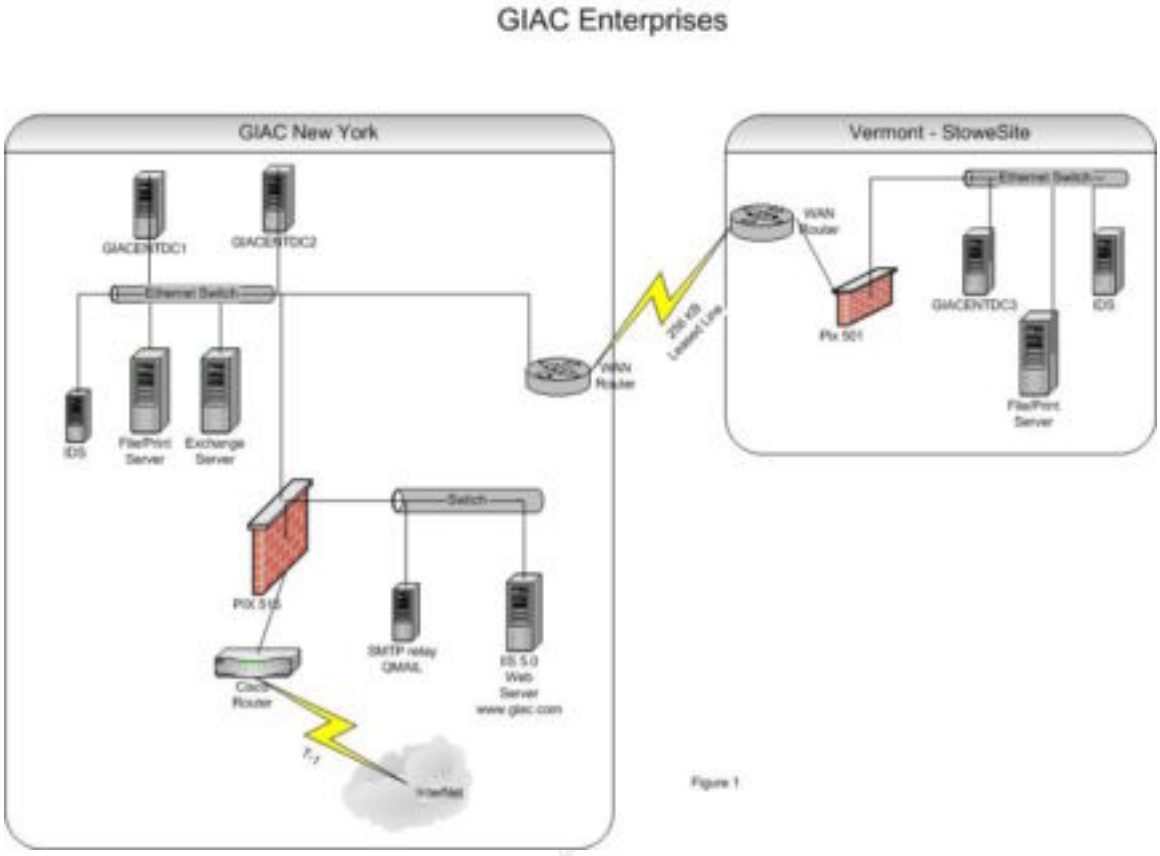
The following security measures have been implemented across the domain:

1) All domain controllers and member servers are in a secure key carded environment.
2) All Windows 2000 computers, member servers and domain controllers have the automatic security update [1]installed. Consequently all patches and service packs are current. All staff have been trained on how to recognize updates and to start the automatic patch process.
3) Further security measures are discussed in the section, *Additional Security.*

New York Headquarters

Figure 1 shows the network configuration for GIAC Enterprises.

[1] http://v4.windowsupdate.microsoft.com/en/default.asp



Domain Controllers

Two domain controllers (GIACENTDC1 and GIACENTDC2) provide Active Directory services for GIAC enterprises. Upon installation the domain was named GIACNET.com. GIACENTDC1 w installed first. As such it adopted all FSMO roles. Upon installation of G2, FSMO operations were shared between the two machines. Table II describes the operations:

Machine	FSMO function	MMC to change operations
GIACENTDC1	Schema Master	Schema Snap-in
GIACENTDC1	Domain Naming Master	A/D Domains and Trusts
GIACENTDC2	Infrastructure Master	A/D Users and Computers
GIACENTDC2	RID Master	A/D Users and Computers
GIACENTDC2	PDC Emulator	A/D Users and Computers

Table II – Domain Controller Functions GIAC Enterprises

Note that while the network runs in native mode, the PDC Emulator is still used in a native environment. [2]

[2] http://support.microsoft.com/default.aspx?scid=kb;en-us;Q197132

In mixed mode the PDC emulator provides:

1) time services for the kerberos protocol
2) preferential management of password changes by other DC's
3) authentication failure (bad password) at other DC's
4) account lock-out
5) replication to BDC's

In a native environment. the PDC Emulator provides:

1) authoritative time service
2) preferential management of password changes by other DC's

Other Services

Table III describes other network functions.

Machine	Function	MMC to change operations
GIACENTDC1	Global Catalog Server	Default install
GIACENTDC2	Global Catalog Server	Default install.
GIACENTDC2	Internal DNS server	Installed as an option during set up
File/Print server	DHCP Server	Installed as an option during set up
GIACENTDC1	Time service	net time /setsntp: ntp2.usno.navy.mil or 192.5.41.209

Table III – Domain Controller Functions GIAC Enterprises

Global Catalog Servers

While it is not recommended to run the Global Catalog Service on the same unit as the infrastructure master *in a multi-domain environment*, it can safely be done in a single domain providing fault tolerance.[3]

DNS Service

The DNS service is installed as *active directory integrated* This feature of 2000 allows for:

1) Multi-master replication among specified alternative DNS servers (one at each site)
2) Incremental updates – updates of only changed records

---

[3] Fossen Active Directory, Group Policy and DNS p. 41

3) Secure updates – only the creating user and the admin can update a host record.
4) Fault tolerance – with A/D all active directory integrated DNS units can receive updates.

The servers are configured to allow only secure updates.

File/Print servers

The file/print server provides storage and printing services to Sales and Marketing. The NTFS permissions on the storage areas have been set to a minimum of *authenticated user* access and where appropriate, only specific user groups within all departments may access storage areas.

DHCP service is provided locally by the file/print server. It is recommended that DHCP not be placed on a DC because of permission problems using the dnsupdateproxy group and ownership of host records [4]

Exchange 2000 server

The Exchange 2000 sits being the firewall in zone security0 (the highest security level). It exchanges email via SMTP (port 25) through the firewall. The firewall rule allows only port 25 between the QMail server's IP and the Exchange server.

Intrusion Detections Systems

A secured Snort intrusion detection system provides alert in the event of firewall circumvention. The snort rules are downloaded and updated regularly. In addition, the snort system provides syslog services for the PIX 515.

The PIX 515 has been configured to do protocol fix-ups and has all IDS signatures enabled. The PIX allows in port 25 TCP for SMTP services to the Exchange server and port 1433 TCP for SQL Server requests.

New York Headquarters - DMZ

SMTP Relay - QMail

The SMTP service on the DMZ is provided by QMail[5], a replacment for sendmail that is designed for security. It runs on a Red Hat 7.2 LINUX with all operating system patches kept current.

[4] IBID, p. 105
[5] http://cr.yp.to/qmail.html

Web Server

Web services, HTTP (80 TCP) and HTTPS (443 TCP) are provided by a Windows 2000 server running IIS 5.0. It is configured following the guidelines described by the NSA [6]

External DNS service is provided by GIAC's Internet Service Provider

New York Headquarters - Outside Zone

Cisco router

The Cisco router provides *defense in depth.* It evaluates ingress and egress traffic and filters via ACL's. Besides routing packets, its defensive functions include:

1) Anti-spoofing
2) Block source routed packets
3) Block private IP address routing
4) Control ICMP communications

The router writes its logs to the Snort syslog server.

WAN Router

Responsible for routing between each of the two sites, it also provides *defense in depth.* It evaluates ingress and egress traffic and filters via ACL's. Besides routing packets, its defensive functions include:

1) Anti-spoofing
2) Block source routed packets
3) Block private IP address routing

The WAN router writes its logs to an Administrators machine.

Stowe Site

The Stowe, Vermont site (StoweSite) houses the R&D department.

Domain Controller

Machine	Function
GIACENTDC3	Global Catalog Server

[6] Walker, Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0®

GIACENTDC3	Domain Name Service
FileServer	DHCP Service

The domain controller is a global catalog server. This function allows a copy of about 55% on the active directory to be stored on-site, preventing unnecessary traffic across the Wan. In the event of a DC failure, a workstation will contact another GC at the remote sites.

Domain Name Service is also provided at this site to cut down on name service lookup requests across the WAN. Clients are configured with secondary and tertiary DNS servers from New York and Burlington.

File/Print server

DHCP service is provided locally by the file/print server. It is recommended that DHCP not be placed on a DC (see previous citation 4).

The File/Print server maintains encrypted folder services for storing prototype fortune designs.

Intrusion Detection Systems

The IDS functions are similar to those of main office. They include the PIX 501 (50 user license) with fixups and IDS functions and the Snort IDS.

Active Directory Design and Diagram

Figure 2 shows the Active Directory Schema FOR GIAC Enterprises.

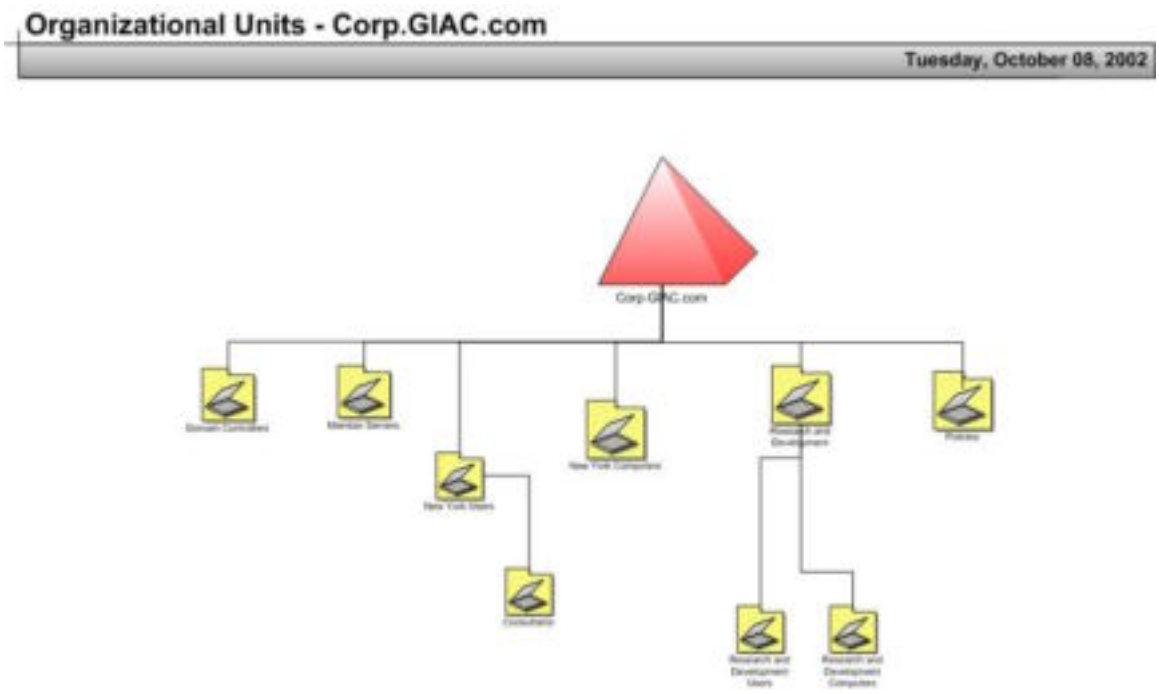


Figure 2

The Active Directory design was chosen based upon the requirements listed in Table IV.

The need for differing policies in R&D
The geographically separate location of the department
The presence of reliable and reasonably high speed network connections
The presence of IT staff at the R&D location
The ability for all network resources at either site to be managed by either IT staff, when necessary.

Table IV – Active Directory Design Requirements and Assets

Domain structure

The Deployment Planning Guide suggests approaching domain design in terms of start with a single domain only, then prove that you need more than one. More or less, “Single domain? Why not?”

A single domain was chosen for GE because:

1) All domain-wide policies are consistent across departments including R&D.

2) There is ample and reliable bandwidth to handle inter-site replication. Additionally, the single domain does not generate enough replication traffic to cause concern about unnecessary replication.
3) A domain can be used to provide autonomous control over the network objects. The requirement for New York to have overriding control over policies precludes the need for autonomous control.

The domain name was chosen as the internal domain name. Recall that all external domain name resolution will be controlled by GE's ISP.

Site Design

A site is an area of well connected IP subnets. A site is used to connect physical locations that have a relatively slow communications link between them. The network designer/administrators can manage directory replication between the two sites by controlling:

1) Schedules – the time of day in which the link is available for replication
2) Cost – the method of determining priorities of various links in use for replication
3) Interval – how frequently a DC is polled for replication changes
4) Transport methods – IP or encrypted SMTP

Given the requirements and assets described in Table IV, Figure 2 shows that the active directory was split into two sites:

1) NewYorkSite (formerly Default First Site)
2) StoweSite

A Domain Controller was placed at StoweSite to localize of Active Directory queries to the onsite controller increasing network performance. Traffic across the private 256K link is limited then to replication of the global catalog as well as user services such as email or hypertext packets.

Inter-site replication occurs every three hours and replication will occur via TCP/IP transport. The Cost, interval and schedule will be default

Organizational units

Following best practice guidelines[7], default Organizational Units were used for the New York site. They were renamed for clarity but the focus of the design was simplicity.

[7] Fossen, Active Directory, Group Policy and DNS p. 60

This structure goes two levels deep, aiding in ease of administration. With fewer levels there is less chance for designing conflicting policies. Additionally performance is enhanced when levels are kept below five deep.

Domain Controllers OU and Member Servers OU

By keeping all domain controllers and member server in a single OU, we may simplify management. All domain controllers and member servers, New York and Stowe, are managed by the policies applied to this OU. These policies are generally broad in nature. More granular management requirements are applied at the OU level.

New York Users OU

All users in the NewYorkSite have the same general software and security requirements. Consequently users from all New York departments were moved into this OU. Additionally a container was created for the Consultant policies. By placing it into the NewYork Users OU, it will inherit their security properties as well as additional properties assign to that child OU.

New York Computers OU

Likewise all New York departments are subsumed under this container.

Policies OU

The policies OU container was created merely as a way to organize any policies that are created. Network Administrators at Stowe or New York may create policies, however they are created in Policies OU and then linked to the appropriate OU.

Research and Development OU

Owing to differences in user requirements an OU was created for the Research and Development. As a smaller unit of GE, there are fewer hours when an administrator can be on-site. Further, the programmers are housed at Stowe and need extraordinary privileges. By creating a separate OU, granting extra privileges may be executed at the OU level. Permissions like resetting passwords are also delegated to the R&D OU that we do not want propagated to the New York Site.

Group Policy and Security

Basic Group Policy

Group Policy objects provide the vehicle for specifying settings for registry-based policies, security settings, *Intellimirror* software installation and maintenance, scripts, folder redirection for users, remote O/S installation services, and Internet Explorer definition and maintenance.

Through the use of Group policy objects, a consistent security environment may be formed. The basic process involved is to define a set of security settings, create a Group Policy object file and then apply that object to a Site, Domain or Organizational Unit. Objects that are applied (linked) to that active directory unit are downloaded and applied at boot or logon time.

Rather than create policies from scratch, third party templates are available for modification to meet GE's needs. NSA provides seminal policies from which GE's security policies are designed. These policies may be downloaded from:

: http://nsa2.www.conxion.com/win2k/

The following files were downloaded, renamed and modified using the MMC snap-in Security Templates.

Download File	Purpose of Template	New File Name
w2k_domain_policy.inf	Domain Policy	GE_Domain.inf
w2k_dc.inf	Domain Controller	GE_DC.inf
w2k_server.inf	Member Server	GE_Server.inf
w2k_workstation.inf	Workstation GPO	GE_Wkstn.inf

When a computer is joined to a GE domain, the local Group policy object settings are applied. Any conflicts arising between the two are overridden by site, domain policy and OU policies in that order.

Default Domain Policy

The Domain policy is configured to control these properties across the entire domain. All Windows 2000 computers (no down level systems are used at GE) systems will receive these policies at power up or logon time.

Password Policy

Passwords *are the first line of defense against interactive attacks on your systems.*[8] A balance must be struck between an oppressive regime of security

[8] Password Assessment and Management, SANS GSEC course

enforcement and a secure network system. The following settings have been applied to the Domain. They are based on Best practice recommendations (Fossen, 2001) [9]

Password Policies	**Setting**
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	5 days
Minimum password length	8 characters
Passwords must meet minimum complexity requirements	Enabled
Store password using reversible encryption for all users	Disabled

Password settings are designed to enforce the structure of passwords that are resistant to dictionary cracks and flexible enough with respect to design requirements as to be easily remembered. Users are taught the general password tricks like choosing a familiar phrase, parsing out the *nth* letter and using that as a pass password. *The Story of Goldilocks and the 3 Bears*, using the 1st letter, becomes the password TSoGat3B.

Enforce Password History:

In order to ensure that passwords aren't reused frequently, eight passwords will be remembered.

Maximum password age

The number of days (90) before a password must be changed.

[9] Fossen, Active Directory, DNS and Group Policy, p.68

Minimum password age

Used in conjunction with password history, prevents users from cycling through 8 passwords immediately to get back to original password.

Minimum password length

Passwords must be at least eight characters. The password complexity requirements will set the minimum at six; hence this setting must be at least six to be meaningful.

Passwords must meet minimum complexity requirements

When this setting is enabled, passwords must meet the requirements defined by Microsoft passfilt.dll including:

- Does not contain all or part of the user's account name
- Is at least six characters in length
- Contains characters from three of the following four categories:
  - English upper case characters (A...Z)
  - English lower case characters (a..z)
  - Base 10 digits (0..9)
  - Nonalphanumeric (For example, !,$#,%)

Should GE choose to tighten the defaults in passfilt.dll, the *Platform Software Developer's Kit* contains tools for revising the default password filter.

Store password using reversible encryption for all users

Reversible encryption is used when one supports Apple® computers. Since GE need not support them and irreversible encryption is insecure, we will ensure that this setting is disabled.

Account Policy

User accounts in the domain may have consistent log-on settings

Account Lockout Policy	**Setting**
Account lockout duration	240 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

The purpose of this policy group is to, at least, slow down brute force attempts at gaining access to a system. Every user has made a typo or become confused about which password to use. The security staff must balance between allowing users to get their work done and preventing denial of services attacks against the system. Users are given a generous number of logon attempts, a relatively short interval for reset and a help staff with the authority to reset passwords.

Account lockout duration

Accounts remained locked for four hours once the account lockout threshold has been met.

Account lockout threshold

Five invalid logon attempts will trigger an account lockout.

It is important to note that failed log-ins against a system locked by CTL+ALT+DEL or by screen saver do not count against those five invalid logon attempts.

Reset account lockout counter after

This setting represents the time that must elapse between failed logon attempts before the logon counter is reset to *0 logon attempts.*

Audit Policy

Audit policies may be differentially activated. The settings recommended by NSA proved to be sufficient and were directly implemented.

Audit Policy	**Settings**
Audit account logon events	Success, Failure
Audit directory service access	No Auditing
Audit logon events	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing

Audit system events	Success, Failure

The focus of auditing will be based upon tracking the activity of attackers. Auditing can be a time-consuming, fairly highly skilled activity. The audit policy will limit the noise through which an administrator must sift.

Audit account logon events

Tracks logon events from local computers participating in the domain. Enable success and failure to track who has tried to log in or has successfully logged in when and where.

Audit directory service access

This setting is sensitive only to A/D objects. Given that the A/D resides only on Domain Controllers, it is best implemented at the domain controller level.

Audit logon events

This setting records the type of logon (interactive, network or service) where the logon occurred. Failures may give us more information about possible intrusion attempts.

Audit policy change

This setting generates a log entry when a change to user rights assignment policies, audit policies, or trust policies is successful or not.

Audit privilege use

Generates an audit event when a user tries to exercise a right for which s/he is not privileged. The entries may give information about a user who is testing the security policies of a system.

Audit system events

This property records events that affect the entire system or the event log.

Security Settings

Additional restrictions for anonymous access	No access without explicit anonymous permissions
Allow system to be shut down without having to log on	Disabled

Allowed to eject removable NTFS media	Administrators
Audit the use of Backup and Restore privilege	Enabled
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign client communication (always)	Disabled
Do not display last user name on logon screen	Enabled
Number of previous logons to cache	0 logons
Message text for users attempting to log on	Warning Message
Message title for users attempting to log on	Warning Title

The focus of the security settings is to make our systems more resistant to general attacks based on access. We start to restrict damage that can be done with physical access and network access.

Additional restrictions for anonymous access

By default an anonymous user has the same access as the everyone group. Changing to this setting prevents enumeration of network shares and domain accounts. *Everyone* and *Network* is removed from the anonymous token preventing a null user enumeration.

Allow system to be shut down without having to log on

A machine can be owned, if physical access is allowed. Preventing shutdown without log on at least slows down an unauthorized user from rebooting to an O/S that overrides our security settings.

Allowed to eject removable NTFS media

Only administrators may eject removable media, preventing theft of desirable information or slowing attacks based on autorun features.

Audit the use of Backup and Restore privilege

Backup and restore use will be audited. This setting will only record failures to the security log as we are not tracking success of privilege use.

Clear virtual memory pagefile when system shuts down

This setting prevents unauthorized individuals from gleaning information from the swap file.

Digitally sign client communication (always)

Mutual authentication is required to help prevent man-in-the-middle attacks in Windows 2000. Given that GE is operating in native mode, these policies will be enforced among all systems. The network designers deemed the trade-off of a 15% hit in performance as reasonable.

Do not display last user name on logon screen

While inconvenient for users, users must enter their User ID as well as their password

Message text for users attempting to log on
Message title for users attempting to log on

Users and would be intruders should not have an expectation of privacy when logging on to GE systems. The legal representatives of GE designed a statement and title to warn users and intruders.

Number of previous logons to cache

This setting will prevent users from logging on using cached credentials. A situation in which a domain controller is unavailable at either site is highly unlikely.

Settings for Event Logs

Maximum application log size	500 MB
Maximum security log size	1000 MB
Maximum system log size	500 MB
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for application log	Overwrite Events As needed
Retention method for security log	Overwrite Events As needed

Retention method for system log	Overwrite Events As needed
Shut down the computer when the security log is full	Disabled

Log settings are based upon generous anticipated storage needs. The security log is allocated more space given the auditing activities configured. While it might be ideal to ask administrators clear log manually, it is not be reasonable. Overwrite events as needed was chosen.

Additional settings from the NSA policy were deemed appropriate for GE's use. Of note were the policies to further lock down registry keys allowing system and administrator accounts full control and users read and execute control.

Domain Controller Policy

The domain controllers inherit policy from the domain policy. The following changes were made to GE_DC.inf to enhance DC security.

Given that a domain controller may be moved from the default domain controller OU, domain controllers inherit certain settings from the domain policy. These policies include:

- Account, Password and Kerberos policy settings
- Rename users and guests
- Automatic logoff when logon time expires.

In addition to the polices inherited form the domain policy, the changes are listed below.

Audit Policy

The following changes were effected by the NSA template. GE chose to retain these settings.

Audit Policy	**Settings**
Audit directory service access	Failure
Audit object access	Failure
Audit process tracking	Failure

Audit directory service access

Whenever an attempt is made (and failed) to alter an LDAP object an event is written to the security log.

Audit object access

Whenever an attempt is made (and failed) to access physical objects such as files, folders, and printers an event is written to the security log.

Audit process tracking

Track the instances of processes that failed while trying to running on the DC. Essentially, it gives administrators information on processes that *ought not* to be failing.

User Rights Assignment

The NSA settings are retained. Administrators are allowed to join *new* computers to the domain and to create shares on the Domain Controllers.

User Rights Policy	**Settings**
Add Workstations to the Domain	Administrators
Create Permanent Shared Objects	Administrators

Add Workstations to the Domain

Only administrators may add computers to the domain.

Create Permanent Shared Objects

Only administrators may set up permanent shares on DC's

Member Server Policy

Member servers inherit most of their settings from the Default Domain Policy. After that the policy GE_Server.inf which is identical to the NSA policy w2k_server.inf is applied.

Web Server Policy

The web server is a standalone Windows 2000 system. It is not joined to the domain and receives its policy locally. This systems runs under the Microsoft High Security Web Policy (hisecweb.inf).

Policies	New Setting	Original Setting
Enforce password history	8 passwords remembered	24 passwords remembered
Maximum password age	30 days	42 days
Minimum password length	12 characters	8 characters
Account lockout setting	3 passwords	5 passwords
Message text for users attempting to log on	Matches domain text	This is a private computer system <add your own text>
Message title for users attempting to log on	Matches domain title	Attention!

While beyond the scope of the current paper, it is important to note that the IIS server has also been configured accord to the guidelines discussed in *Securing Internet Information Server*[10].

Workstation Policy

Once again, the preponderance of security settings are obtained form the default domain policy. The NSA settings are retained. The focus of these policies is to provide more usability at the workstation level

Event Logs

Smaller event logs are likely to be appropriate given smaller disk capacity and *less interesting* resources.

Maximum application log size	125 MB
Maximum security log size	250 MB
Maximum system log size	125 MB

Security Settings

A number of employees use laptops. It is advantageous to log in to the domain when disconnected from the network. The minimum of one cached user is set.

[10] Fossen, *Securing Internet Information Server*

Number of previous logons to cache	1 logons

User Rights Assignment

Authenticated Users are a system group that excludes anonymous access from its membership. Users will have the ability to perform these additional operations.

User Rights Policy	**Settings**
Log on locally	Authenticated users
Shut down the system	Authenticated users
Create permanent shares	Authenticated users
Allowed to eject removable NTFS media	Authenticated users

Additional Group Policy

Workstation Policy linked to the Research and Development OU

The R&D OU contains the programmers. These individuals have additional needs for testing and debugging the fortune generator system. Consequently, they are given these privileges in a policy named *ProgrammerPolicy*.

Audit Policy

Programmers will need the ability to watch the processes their programs spawn. Unlike humans, programmers will be interested in the successful behavior of their code as well as its unsuccessful behavior.

Audit Policy	**Settings**
Audit process tracking	Success, Failure

Event Logs

Larger event logs are needed for the directory service

Maximum application log size	500 MB
Maximum security log size	500 MB
Maximum system log size	500 MB

User Rights Assignment

Authenticated Users are a system group that excludes anonymous access from its membership. Users will have the ability to perform these additional operations.

User Rights Policy	**Settings**
Allowed to eject removable NTFS media	Programmer
Debug programs	Programmer
Profile system performance	Programmer
Allow logon as services	Programmer
Manage auditing and security log	Programmer

Consultant Policies

Consultants are transient users working for the marketing staff. The focus of the consultant policy is to restrict their configuration capability, *slow* their ability to access CMD.EXE and to preserve their work on a shared folder.

A GPO will be applied to the Consultant OU with these properties. There is an option to apply the policy to a group. Since only consultants are placed in that OU, the policy will be applied to all users.

Policy	**Settings**
Disable Control Panel	Enable, All users
Remove Run menu from Start Menu	Enable, all users
Disable the command prompt	Enable, all users

Disable Task Manager	Enable, all users
Disable registry editing tools	Enable, all users
Application Data	\\GEFileServer1\%username%
My Documents	\\GEFileServer1\%username%

Disable Control Panel

User Configuration\AdministrativeTemplates\Start Menu & Taskbar

Consultants will have the control panel disabled. Any configuration that is needed from within the control panel may be performed by an administrator

Remove Run menu from Start Menu

User Configuration\AdministrativeTemplates\Start Menu & Taskbar

Disable the command prompt

User Configuration\Administrative Templates\System

Disable Task Manager

User Configuration\Administrative Templates\System\Logon/Logoff

These three policies will prevent many users from getting to a command prompt. Disabling task manager prevents a user from starting a process from the task manager. The other two prevent running CMD.EXE from Start=>Run and from Start=>Programs=>Accessories, respectively.

Disable registry editing tools

User Configuration\Administrative Templates\System

Application Data and My Documents

User Configuration\Windows Settings\Folder Redirection

Application data are folders in which a software vendor may store program customizations, such as personal additions to the spell checker or preferences. My documents is the default folder for storing saved work in many applications.

Consultants are instructed to store all data in *My Documents*. It is explained that this folder is backed up nightly, preserving the work for which GE has paid them. Further, they are instructed not to save work locally.

Managing the Encrypted File System

The most concise explanation of the encrypted file system process comes from the *SANS Securing Windows 2000 Step-by-Step Guide*[11],

> Windows 2000 encrypts with a randomly chosen File Encryption Key. This key is then encrypted with the user's Public key for safekeeping. In the event that the encrypted files need to be decrypted by a system administrator in an organization, that File Encryption Key is also encrypted with the public key of the Recovery Agent. Computers that are members of an Active Directory Domain have the domain Administrator account as the default Recovery agent…

Should the private key become corrupt, presumably valuable files become unusable. Use the Certificates MMC to backup the key to diskette, secure the key with a password and lock up both password and key diskette in separate locations.

Policy OU

The policy OU simply serves as a container for all policies. Any new polices are created in the policy OU. Its sole purpose is to provide a list of all policies for any administrator wishing to see the list. While one may search for policies, it is a convenience and a standard.

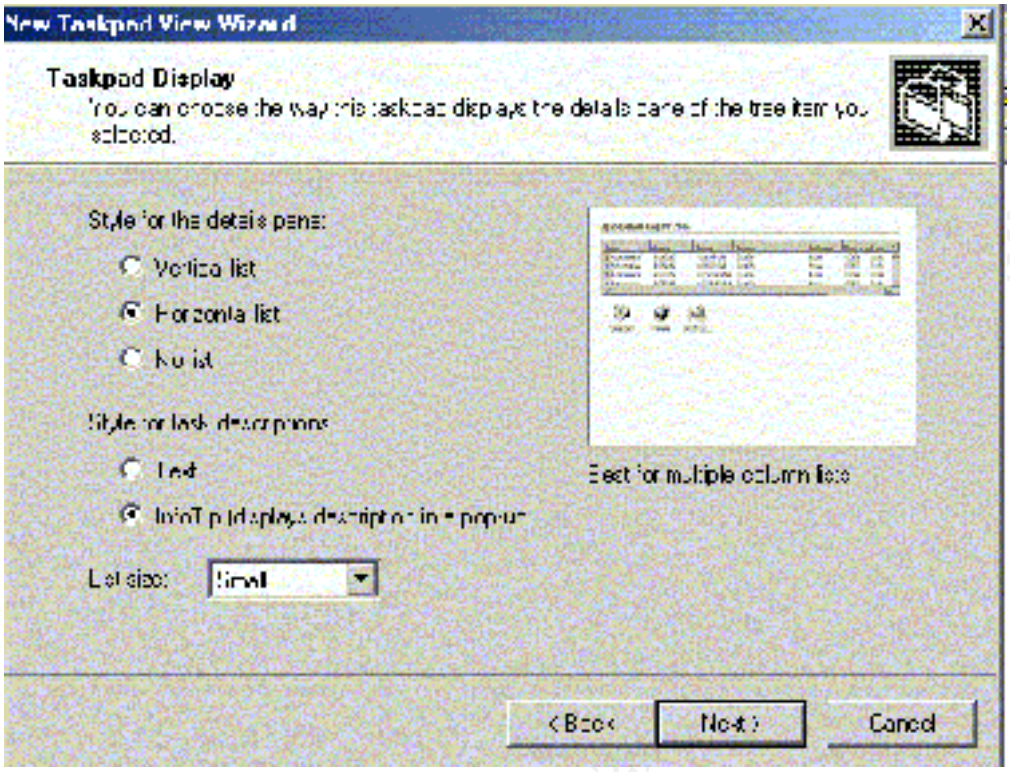
Password Resetting for Stowe Site

One of the network goals is to allow non-technical users the privilege to reset passwords. A small group of users, PasswordResetters has been created and selected user accounts have been placed in that group.

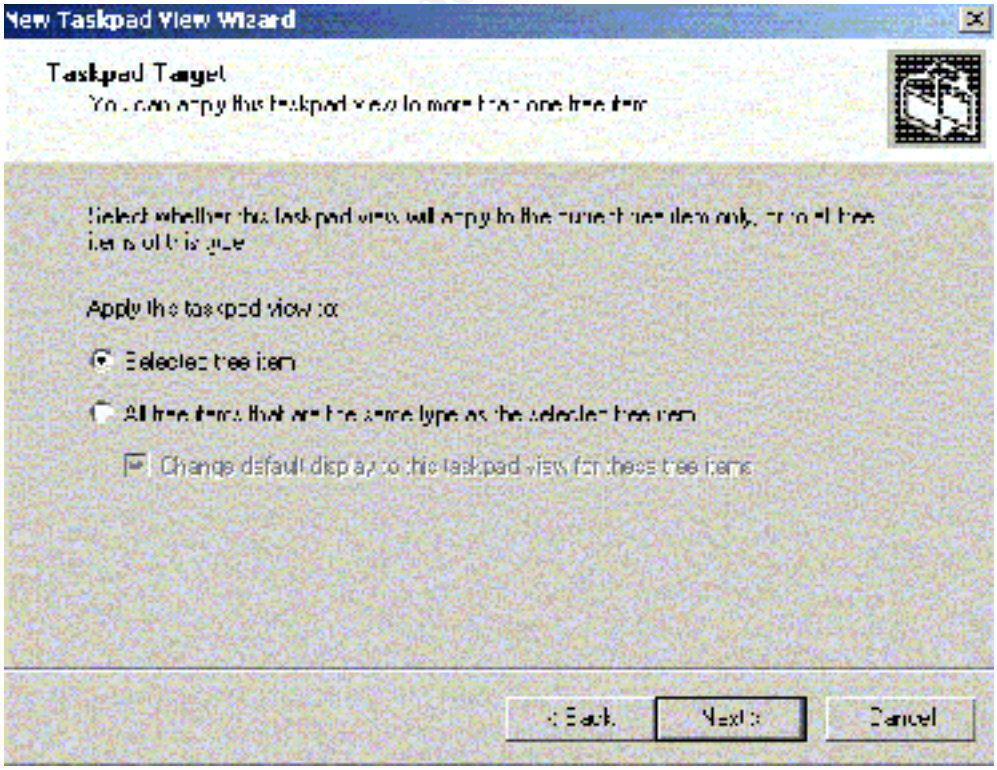
These process of creating the *taskpad* view is:

1) Having opened an instance of the MMC *Active Directory Users and Computers*, the *Research and Development Users OU* should be selected.
2) Right click the OU and selected open *new window from here*.
3) Right click the *Research and Development Users OU* and select the *New Taskpad View* to launch the wizard.
4) Answer the questions regarding style

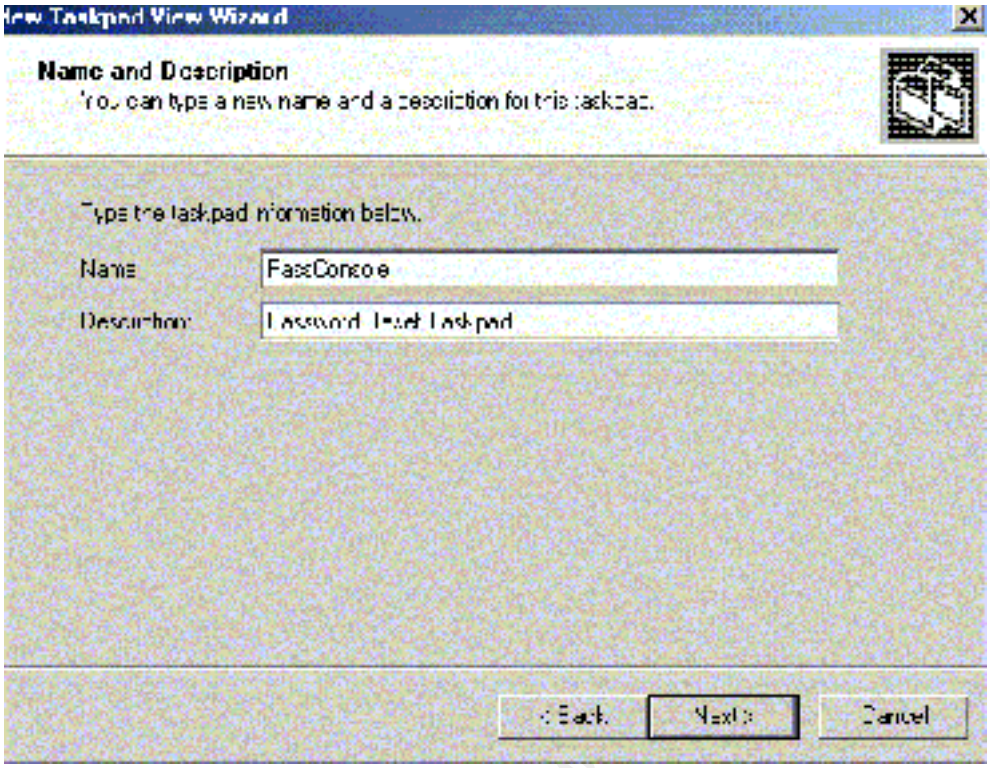
[11] Shawgo, p. 17



5) Select *Selected Tree Items* to limit its functions.



6) Name the console, click next

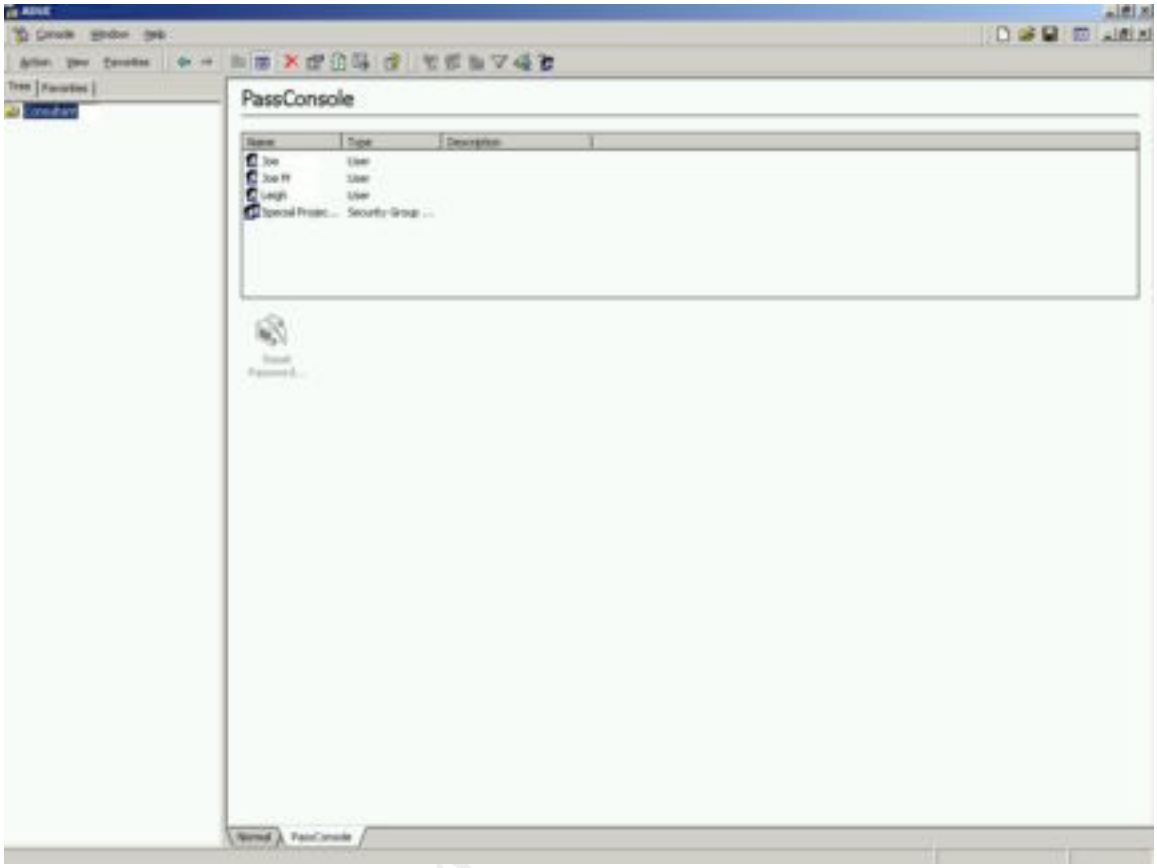


7) Ensure that *Start the New Task Wizard* is selected before finishing. .

8) On the new task wizard Click past *Menu* command

9) Choose *Reset Password.* And select an icon.

10) Complete the task wizard. The console will look rather like this



With the task pad, a user is selected and the password is reset to a value shared with the user.

The taskpad will be deployed to a folder with NTFS shares set for administrators (full) and for PasswordResetters (read).

In order for the taskpad to function, the user must have the *Active Directory Users and Computers* snap-in installed on his/her workstation. Consequently, we do not want these people to have the authority to link GPO's to Active Directory objects. Minimally, these trusted but non-technical users should not be members of the Domain Administrators or Enterprise Administrators group.

While not implemented in this design, it is important to note that groups may be restricted to only certain snap-ins by the use of group policy. They may be allowed or denied specific snap-ins through:

User Configuration\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins

Additional Security

Network Defense in Depth

A synergy exists when multiple levels of defense are integrated into a network. Windows 2000 represents a major improvement in terms of ease of securing a system. It cannot complete by itself. These countermeasures add to the GE network security.

NTFS perms for Programmer and for Consultant

Microsoft structured groups in the following method. The mnemonic is AGUDLP or AGDLP

Users are **added** to the active directory
Then assigned to **G**lobal Groups
Global groups are placed in **U**niversal group (if necessary)
Global Groups are placed in **D**omain **L**ocal groups
Permissions are assigned to domain local Groups

Use r accounts for programmers are added to the global group ggProgrammer.
The ggProgrammer group is added to the dlProgrammer group
The programmer group then receives its additional privileges in the context of the GPO applied to the R&D OU

Virus Scanning

Anti-virus software is installed on each workstation and server at installation time. Automatic updates are pushed out to machines and machines are scheduled to scan once weekly.

The exchange server monitors incoming email for virus checking as well.

Malware

A major source of malware comes from unauthorized downloads. Peer-to-Peer technologies like KaZaA are infamous as a portal for viruses and Trojan horse programs. Additionally, it installs software to presents ads and to report the user's surfing habits.

Countermeasures have been set up. Users in the User Group have no registry rights to install software. If a download requires a registry change, the user cannot install it.

The intrusion detection software located at each site can also monitor suspicious ports (e.g. 1214) and identify workstations engage in undesired activity.

Intrusion Detection
The snort signatures [12] are used to alert the network monitor of suspicious behavior. Alerts range from virus signatures, trojan port usage and port scans

Log Analyses

Logs provide an important source of threat analysis. In addition to the security log, information provided by the PIX firewalls and the router can add to an attack profile.

Social Engineering

The ability for an individual to trick users and administrators into divulge passwords or information about systems. Educating users, helpdesk and even administrators to typical social engineering scams is helpful. Providing clear written guidelines outlining procedures for password resetting will mitigate difficult situations. Having central contact points for fielding questions regarding system information will also minimize risk.

Network Physical Security

Physical access to a machine equals a compromised machine/network. Rebooting a system into *NIX will prevent the most well planned NTFS policies and perms. People should be trained to *assist* unknown individuals to a receptionist when found wandering the halls or when found in a cubicle.

All network hardware and cabling should be secured behind locked doors, out of the way in ceilings. Switch ports should be restricted to MAC addresses or shut off. Cables not connected to PC's should be disconnected at the switch. Older firmware should be updated to patch security holes.

Disaster Recovery Plans

Regular backups must occur. They must be tested on a regular basis. Tapes must be stored in a secure spot on-site. Tapes should be stored in a secured off site location as well. They must be rotated in and out on a regular basis. Tapes must be replaced at a regular interval to prevent failure.

Plans must be made for hardware replacement in the case of a failure

[12] www.snort.org

Patch Application

Microsoft has made a fine effort to push patches and service packs out to machines automatically via GPO's and .msi files. All server at GE are running the automatic update alerter program. This program notifies administrators/user when their machine have an appropriate patch available.

On a tangential note, the .NET initiative has the possibility of providing automatic updates for custom written software. Updates may likewise be rolled out without administrator intervention. Since software can also run server-side, software is updated at the server only, saving many steps/visits to client machines.

All administrators have subscribed to the better security bulletin services including:

- www.microsoft.com/security/
- www.sans.org
- www.securityfocus.com

Conclusions

The network design goals outlined at the beginning of this document were met.

1) Network structure and, consequently, management will be as simple as possible.

   Whenever possible, default objects were used. A minimum number of Policies and OU's were created. The Stowe site was designed to minimize replication traffic with a domain controller and onsite DNS.

2) All workstations and users must be secured. Research and Development has different security requirements than the other departments.

   Workstations were secured primarily via domain wide policy and additional workstation policy.

3) Management of security policies may be implemented by IT staff at each of the two sites. However, the default domain policy is immutable.

.

   By ensuring that the no override property of the domain policy is set, a given administrator cannot implement a conflicting policy accidentally. While any administrator may change the domain policy, each person is equally trusted in this small organization.

4) Consultants, who are employed on occasion, have additional constraints for network use.

   A consultant OU was created with a policy to restrict certain workstation functions was created. All consultant users were moved into that OU.

5) Certain non-IT departmental staff will be asked to perform some of the less technical network management tasks.

   A taskpad, was created for the *Research and Development Users OU*. The necessary snap-ins were applied to the user's computers and appropriate rights were given to the folder containing the taskpad view.

References

Microsoft Corporation. “How To Delegate the Unlock Account Rights (Q294952).” URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q294952 (18 April 2002).

Microsoft Corporation. “Keeping Group Policies from Applying to Administrator Accounts” URL:http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315675

Microsoft Corporation. “Passwords must meet complexity requirements of the installed password filter.” URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/504.asp (18 April 2002).

Microsoft Corporation. “User Data and Settings Management, White Paper” URL: http://www.microsoft.com/windows2000/techinfo/administration/management/settings.asp (31 July 2000)

Microsoft Corporation. “Windows 2000 Group Policy, White Paper”. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp (31 July 2000)

Microsoft Corporation. Windows 2000 Active Directory FSMO Roles”. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q197132 (10 Dec. 1998)

Microsoft Windows 2000 Server Deployment Planning Guide. Redmond WA:Microsoft Press, 2000

Bernstein, D. J. “qmail download site”. URL:http://cr.yp.to/qmail.html

Cole E., Kolde, J.“Password Assessment and Management, Security Essentials”.The SANS Institute GSEC Course.

Fossen Jason. “Active Directory, Group Policy and DNS” The SANS Institute, August 2001.

Fossen, Jason. “Securing Internet Information Server 5.0” The SANS Institute Course. 31 October 2001.

Fyfe, Bruce. **“**Building a Secure Windows® 2000 Professional Network Installation. A Best Practices Approach to Securing a Windows® 2000 Networked Workstation.” URL: http://rr.sans.org/win2000/net_install.php (24 Apr. 2002)

Haney, Julie M. "Guide to Securing Microsoft Windows 2000. Group Policy Network Security Evaluations and Tools. Division of the Systems and Network Attack Center (SNAC)" URL: http://nsa2.www.conxion.com/win2k/download.htm (13 Sept 2001)

Shawgo, Jeff, ed. "Windows 2000 Security. Step by Step. A Survival Guide for Windows 2000 Security." The SANS Institute. Version 1.5. 1 July 2001

Walker, William, E. IV. "Network Applications team of the Systems and Network Attack Center. Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0®".
URL: http://nsa2.www.conxion.com/win2k/download.htm (4 Mar. 2002)